

AKIN GUMP  
STRAUSS HAUER & FELD LLP

Attorneys at Law

PHIL MARCHESIELLO  
202.887.4348/fax: 202.887.4288  
pmarchesiello@akingump.com

March 27, 2009

VIA ECFS

Ms. Marlene H. Dortch  
Office of the Secretary  
Federal Communications Commission  
455 12th Street, SW  
Suite TW-A325  
Washington, DC 20554

Re: **EB Docket 06-36**  
**Annual 47 C.F.R. § 64.2009(e) CPNI Certification**  
**Interface Security Systems Holdings, Inc.**

Dear Ms. Dortch:

On behalf of Interface Security Systems Holdings, Inc. ("Interface"), please find attached hereto a customer proprietary network information ("CPNI") compliance certification and accompanying statement for filing in the above-referenced docket. Interface filed a CPNI certification and accompanying statement on November 4, 2008 ("November Filing") in the expectation that it would commence providing voice over Internet protocol ("VoIP") services prior to that date. (However, Interface did not begin installing and providing services until December 2008.) Interface's November Filing is sufficient to comply with Section 64.2009(e) of the Commission's rules, 47 C.F.R. § 64.2009(e), which requires companies to file CPNI certificates for 2008 no later than March 1, 2009.

Nevertheless, to the extent that the Commission determines that the November Filing is not sufficient to comply with Section 64.2009(e) for 2008, Interface is hereby filing, out of an abundance of caution, an additional CPNI certification covering all of 2008 and is seeking a waiver of the March 1 filing deadline. The Commission may waive its rules for good cause when the facts of a particular case make adherence to the rule inconsistent with the public interest, inequitable or unduly burdensome. *See* 47 C.F. R. § 1.3; *see WAIT Radio v. FCC*, 418 F.2d 1153, 1159 (D.C. Cir. 1969), *appeal after remand*, 459 F.2d 1203 (D.C. Cir.), *cert. denied*, 409 U.S. 1027 (1972); *see also Northeast Cellular Tel. Co. v. FCC*, 897 F.2d 1164 (D.C. Cir. 1990). In this instance, Interface demonstrated its good faith efforts to comply with the Commission's CPNI certification requirements by submitting the November Filing concurrently with Interface's initiation of VoIP services. Further, because Interface established CPNI compliance procedures prior to its initiation of service and those procedures have been effective to protect its customers' CPNI, the objectives of the Commission's CPNI requirements have been fully satisfied by Interface. Therefore, strict enforcement of the certification filing deadline, to

Ms. Marlene H. Dortch  
March 27, 2009  
Page 2

the extent that the Commission determines that Interface has not complied with such deadline, is inconsistent with the public interest. This is especially true in light of Interface's November Filing and in light of the complex administrative burdens imposed by the myriad of federal, state, and local regulatory issues facing new and competitive entrants into this market, such as Interface .

Please do not hesitate to contact the undersigned with any questions about this matter.

Sincerely,

A handwritten signature in black ink, appearing to read "Phil Marchesiello", with a long horizontal flourish extending to the right.

Phil Marchesiello, Esq.  
*Counsel for Interface Security  
Systems Holdings, Inc.*

Enclosures

**ANNUAL 47 C.F.R. § 64.2009(E) CPNI CERTIFICATION**

**EB Docket 06-36**

Annual 64.2009(e) CPNI Certification for 2008

Date filed: March 27, 2009

Name of company covered by this certification: Interface Security Systems Holdings, Inc.

Form 499 Filer ID: 827355

Name of signatory: Dan Reynolds

Title of signatory: VP of Customer Operations

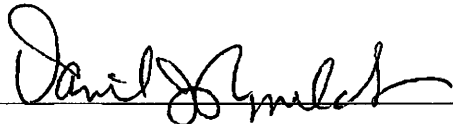
I, Dan Reynolds, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. § 64.2001 et seq. The company began installing, servicing and providing VoIP services on a resale basis beginning in December 2008 and the attached CPNI operating procedures have been in place since that time in compliance with the Commission's CPNI rules.

Attached to this certification is an accompanying statement explaining how the company's procedures will ensure that the company is in compliance with the requirements set forth in section 64.2001 et seq. of the Commission's rules.

The company only began deployment of VoIP services to commercial customers this past December, and therefore, the company has not yet taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

In addition, the company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, e.g., instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).

Signed

A handwritten signature in black ink, appearing to read "Dan Reynolds", written over a horizontal line.

## CPNI POLICY STATEMENT

1. Interface Security Systems Holdings, Inc. (the “Company”) uses or discloses customer proprietary network information (“CPNI”) solely for the purpose of providing voice over internet protocol (“VoIP”) services to which customers have subscribed. Specifically, the Company uses CPNI to initiate and provide VoIP services and to bill and collect payment for such services.
2. The Company may use, disclose or permit access to CPNI (i) to protect its rights or property, or to protect customers and other carriers from fraudulent, abusive, or unlawful use to the services, (ii) pursuant to a valid request from law enforcement, the federal judiciary or other appropriate governmental authority (CPNI will only be disclosed after the requesting party demonstrates that the request is made pursuant to a valid subpoena, court order, search warrant or letter from a national security agency) or (iii) upon receipt of express customer approval to release or disclose the customer’s CPNI to a third party. The Company maintains records of all instances where CPNI was disclosed for any of the foregoing reasons and maintains such records for one year.
3. The Company does not use or disclose CPNI to market any services, regardless of whether customer consent is required for such marketing activities. In addition, the Company does not use or disclose CPNI for any other purpose for which customer consent is required. Because the Company does not use or disclose CPNI for sales or marketing purposes, it is not required to maintain records as specified in Section 64.2009(b) of the FCC’s rules.
4. The Company enters into contractual arrangements with its business customers pursuant to which it provides a dedicated account representative to each business customer, such that business customers are not required to contact the Company’s call center to reach a customer service representative. The Company’s contracts with its business customers also address expressly the Company’s protection of the business customers’ CPNI.
5. Prior to disclosing any CPNI, the Company authenticates its non-business customers in accordance with the FCC’s rules. Specifically, the Company requires its customers to establish an account password and shared secret at the time service is initiated. Neither the password nor the shared secret may be based upon readily available biographical information, *e.g.*, social security number, mother’s maiden name, etc.
6. The Company does not release any call detail information to customers during a customer-initiated telephone call except to the extent (i) the customer provides the Company with a pre-established password or, if the customer has forgotten his password, provides the Company with a correct response to a shared secret; (ii) the customer has requested the Company to send call detail information to the customer’s address of record; or (iii) the Company first places a return call to the customer’s telephone number of record.
7. The Company does not release any call detail information over the Internet unless a customer provides a valid password. In addition, the Company locks a customer account if a user attempts to access an account without the appropriate password three times in a single session.

8. The Company does not release CPNI at any retail location.
9. The Company notifies customers via mail to the customer's address of record whenever an address or telephone number of record is changed, or whenever a password, online account, or customer response to a shared secret is created or modified.
10. The Company trains its employees with respect to the FCC's rules governing CPNI and as to when employees may or may not disclose CPNI. Violation of the Company's CPNI policies may result in disciplinary action, up to and including termination of employment.
11. The Company has implemented procedures to ensure that the United States Secret Service and the Federal Bureau of Investigation are notified of breaches of CPNI as soon as practicable and in no event later than seven days after the Company determines that a breach has occurred. In the event of a breach, the Company will maintain appropriate records in accordance with FCC rules.